REMARKS

The Examiner has objected to the drawings. Drawing corrections have been submitted herewith.

The Examiner has rejected Claims 7, 10, 21, 23, and 25 under 35 U.S.C. 101 because such claims are drawn to computer program products and computer codes, but are not claimed as embodied in computer-readable media. Such rejection is overcome, however, in view of the clarifications made hereinabove.

The Examiner continues by rejecting Claims 1-21, and 28 under 35 U.S.C. 102(e) as being anticipated by Ranger (USPN 6,393,568). Applicant respectfully disagrees with this rejection, especially in view of the amendments made hereinabove. For example, applicant has cancelled Claims 19-21.

Further, the Examiner relies on the following excerpt from Ranger to make a prior art showing of applicant's claimed "identifying a process for accessing files" (see Claims 1, 7, 13, and 28).

> "A computer based encryption and decryption system is disclosed which provides content analysis through a content inspection mechanism, such as detection of a computer virus using a virus detection mechanism, based on determining whether digital input information is encrypted." (see col. 2, lines 25-28)

Such excerpt, however, merely suggests identifying whether a file is encrypted or not, so that the file can be decrypted prior to scanning. There is simply no disclosure, teaching or even suggestion of any sort of identification of "a process for accessing files." Applicant respectfully asserts that the determination of whether a file is encrypted or not (i.e. the state of file) in no way suggests the identification of a process that is accessing the file. Only applicant teaches and claims a technique for tailoring virus detection actions based on processes that access files.

Despite this clear distinction already present in the claims and in the spirit of expediting the prosecution of the present application, applicant now claims:

> "wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files" (see this or similar language in each of the independent claims).

Applicant thus further distinguishes Ranger by emphasizing the fact that the presently claimed invention is capable of identifying an application program (i.e. a network browser application or a word processor application) that is attempting to access a file, and tailoring the virus detection actions in view of the access attempt by such specific application program. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Applicant further notes that the Examiner's application of the prior art to the dependent claims is also replete with deficiencies. Just by way of example, with respect to Claims 2, 8, and 14, the Examiner states that Ranger teaches the use of a cryptographic application and virus detection application. While this may be true, Ranger simply does not suggest "identifying a process for accessing files" (for the reasons set forth hereinabove), let alone identifying a process for accessing files, where "the process is carried out by an executable file." Again, Ranger suggests the identification of the state of an accessed file (i.e. encrypted or not), not identifying the executable file-initiated process that is accessing the file.

It is further noted that the Examiner has not even attempted to make a specific prior art showing of the subject matter of Claims 3 and 4 et al. See below:

> "wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category" (see Claim 3 et al.); and

"identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files" (see Claim 4 et al.).

Again, a notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

The Examiner has rejected Claims 22-27 under 35 U.S.C. 103(a) as being unpatentable over Ranger (USPN 6,393,568) in view of Ji (USPN 5,623,600). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove (note foregoing remarks). Further, applicant has cancelled Claims 22-23.

Moreover, it appears that the Examiner has not made a prior art showing of applicant's claimed: "defining a plurality of extensions indicative of different types of files based on a user" and "performing virus detection actions on the file based on whether the extension is defined by the user" (see Claims 24-25, and 27). A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested

Still yet, applicant brings to the Examiner's attention new Claim 29 below, which is deemed to be novel:

"(a) identifying a process for accessing files;

(b) selecting virus detection actions based at least in part on the process; and

(c) performing the virus detection actions on the files;

wherein the process is identified from a plurality of processes each carried out by an executable file, the processes initiated by application program-related executable files including FindFast.exe, WinWord.exe, and Explorer.exe, for tailoring the virus detection actions when attempts are made to access the files;

wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category;

wherein the process is identified by inspecting a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the identified process, and a user of the process."

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P004/00.006.01).

Respectfully submitted,
Silicon Valley IP Group, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100